(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平8－251156

(43)公開日　平成８年(1996)９月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06			Ｈ０４Ｌ	9/02	Ｚ
	9/14		7368－5Ｅ	Ｇ０６Ｆ	13/00	３５１Ｚ
Ｇ０６Ｆ	13/00	３５１	7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｇ０９Ｃ	1/00		9466－5Ｋ	Ｈ０４Ｌ	11/20	１０１Ｂ
Ｈ０４Ｌ	12/54					

審査請求　未請求　請求項の数13　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平7－52252

(22)出願日　平成７年(1995)３月13日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　西岡　玄次
神奈川県川崎市麻生区王禅時1099番地株式会社日立製作所システム開発研究所内

(72)発明者　宮崎　聡
神奈川県川崎市麻生区王禅時1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

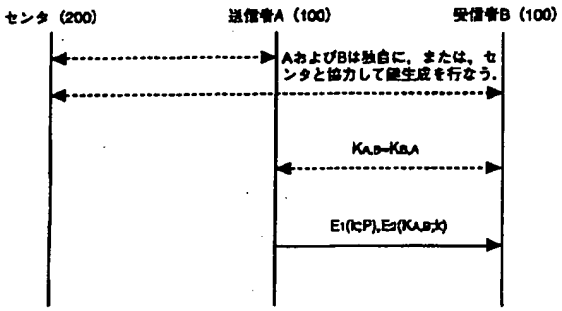
(54)【発明の名称】　電子メール暗号化方法及び暗号化システム

(57)【要約】

【目的】メールシステムや機種に特定しないで通常のメールと併用することができ、電子メールの送信者および受信者双方のセキュリティ機能実現のための計算処理およびメモリの負担が少なく、かつ、利用者の鍵の一致の心配がない盗聴や不正者のなりすましに対して安全性の高い電子メール暗号化方法を提供する。

【構成】通信ネットワークの各利用者は各々の鍵情報を作成し、公開鍵のみを公開する。次に、電子メールの送信者および受信者はそれぞれ自分の秘密鍵と相手の公開鍵からマスタ鍵$K_{A,B}$、$K_{B,A}$の共有を行ない、送信者は秘密鍵暗号を用いて、メール本文Ｐをデータ暗号化鍵ｋで暗号化し、データ暗号化鍵をマスタ鍵で暗号化し、それらを受信者に送り、受信者はマスタ鍵$K_{B,A}$を用いてデータ暗号化鍵ｋを復号化し、さらにデータ暗号化鍵ｋからメール本文Ｐを復号化する。

図 2



1

【特許請求の範囲】

【請求項1】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、送信者Aは秘密鍵x_Aおよび秘密鍵x_Aに対応する公開鍵v_Aを作成し、受信者Bは秘密鍵x_Bおよび秘密鍵x_Bに対応する公開鍵v_Bを作成し、それぞれ公開鍵のみを公開し、マスタ鍵共有処理として、送信者Aは自分の秘密鍵x_Aと受信者Bの公開鍵v_Bからマスタ鍵$K_{A,B}$を作成し、受信者Bは自分の秘密鍵x_Bと受信者Bの公開鍵v_Aからマスタ鍵$K_{B,A}$を作成し、このとき、$K_{A,B}=K_{B,A}$が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵、または、各マスタ鍵を送信者Aの秘密鍵から作成した鍵を用いて暗号化した情報を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし、メール本文の暗復号化処理として、送信者Aはデータ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文$E_1(k;P)$と、データ暗号化鍵kをマスタ鍵$K_{A,B}$にて暗号化した暗号文$E_2(K_{A,B};k)$を受信者Bに送信し、受信者Bは、マスタ鍵$K_{B,A}$を用いて$E_2(K_{A,B};k)$からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いて$E_1(k;P)$からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項2】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、センタはセンタの秘密情報として1対1関数fを作成し、送信者Aは秘密鍵x_Aおよび秘密鍵x_Aに対応する公開鍵y_Aを作成し、受信者Bは秘密鍵x_Bおよび秘密鍵x_Bに対応する公開鍵y_Bを作成し、センタへの登録処理として、送信者Aおよび受信者Bは自分のID情報をセンタに登録し、センタはセンタの秘密情報である関数fを用いて、送信

$$y_{Aj}=\exp(a:x_{Aj})\pmod p \quad \text{for } j=1,\cdots,n,$$

を計算し、y_{Aj}（$j=1,\cdots,n$）を送信者Aの公開鍵として登録し、

受信者Bは、$0<x_{Bj}<p-1$なる整数x_{Bj}（$j=1,\cdots,n$）を

$$y_{Bj}=\exp(a:x_{Bj})\pmod p \quad \text{for } j=1,\cdots,n,$$

を計算し、y_{Bj}（$j=1,\cdots,n$）を受信者Bの公開鍵として登録し（ただし、$\exp(a:x)$はaをx乗した値を表わす）、マスタ鍵共有処理として、

送信者Aは、自分の秘密鍵である整数x_{Aj}と受信者Bの

$$K_{A,B}=\prod\{\exp(y_{Bj}:x_{Aj})\pmod p \mid j=1,\cdots,n\},$$

2

＊者AのID情報I_Aから送信者Aに固有の秘密鍵s_Aを、$s_A=f(I_A)$，で作成し、同様に受信者BのID情報I_Bから受信者Bに固有の秘密鍵s_Bを、$s_B=f(I_B)$，で作成し、センタは秘密鍵s_Aとs_Aに対応する公開鍵v_Aの組（s_A，v_A）を送信者Aに安全に配布し、同様に秘密鍵s_Bとs_Bに対応する公開鍵v_Bの組（s_B，v_B）を受信者Bに安全に配布し、このとき、$I_A\neq I_B$ならば$s_A\neq s_B$かつ$v_A\neq v_B$，が成立し、送信者Aは（y_A，v_A）を、受信者Bは（y_B，v_B）をそれぞれ自分の公開情報として登録し、マスタ鍵の共有処理として、送信者Aは自分の秘密鍵（x_A，s_A）と受信者Bの公開鍵（y_B，v_B）からマスタ鍵$K_{A,B}$を作成し、受信者Bは自分の秘密鍵（x_B，s_B）と受信者Bの公開鍵（y_A，v_A）からマスタ鍵$K_{B,A}$を作成し、このとき、$K_{A,B}=K_{B,A}$が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵、または、各マスタ鍵を送信者Aの秘密鍵から作成した鍵を用いて暗号化した情報、を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし、メール本文の暗復号化処理として、送信者Aはデータ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文$E_1(k;P)$と、データ暗号化鍵kをマスタ鍵$K_{A,B}$にて暗号化した暗号文$E_2(K_{A,B};k)$を受信者Bに送信し、受信者Bは、マスタ鍵$K_{B,A}$を用いて$E_2(K_{A,B};k)$からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いて$E_1(k;P)$からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項3】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、送信者Aは、$0<x_{Aj}<p-1$なる整数x_{Aj}（$j=1,\cdots,n$）をランダムに選び、公開情報である整数a、素数pを用いて、

【数1】

$$y_{Aj}=\exp(a:x_{Aj})\pmod p \quad \text{for } j=1,\cdots,n, \qquad \cdots(\text{数1})$$

※…，n）をランダムに選び、

【数2】

$$y_{Bj}=\exp(a:x_{Bj})\pmod p \quad \text{for } j=1,\cdots,n, \qquad \cdots(\text{数2})$$

公開鍵であるy_{Bj}（$j=1,\cdots,n$）を用いて、マスタ鍵$K_{A,B}$を、

【数3】

3

にて作成し、
受信者Bは、自分の秘密鍵である整数x_{Bj}と送信者Aの公開鍵であるy_{Aj}（j＝1，…，n）を用いて、マスタ＊鍵$K_{B.A}$を、

$$K_{B.A}=\prod\{\exp(y_{Aj}:x_{Bj})\pmod p \mid j=1,\cdots,n\},$$

にて作成し、
このとき、$K_{A.B}=K_{B.A}$が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合S_A、または、送信者Aの秘密鍵である整数x_{Aj}（j＝1，…，n）と鍵生成関数θから、
【数5】$K(A)=\theta(x_{A1},\cdots,x_{An})$，
にて作成した鍵K（A）を用いてマスタ鍵の集合S_Aを暗号化した
$C(A)=E_A(K(A);S_A)$，
を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、$E_A(k;M)$はAが所持する秘密鍵暗号アルゴリズムにより平文Mを鍵kにて暗号化した結果を表わす）、
メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E（k；P）と、データ暗号化鍵kをマスタ鍵$K_{A.B}$にて暗号化した暗号文$E(K_{A.B};k)$をメール受信者Bに送信し、受信者Bは、マスタ鍵$K_{B.A}$を用いて$E(K_{A.B};k)$からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE（k；P）からメール本文Pを復号化することを特徴とする電子メール暗号化方法。
【請求項4】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、
準備処理として、センタは、素数p_1と、p_2-1が二つの大きな素数を因数として持つ素数p_2と、整数a_1，a_2を公開し、p_2-1の素因数分解を秘密とし、送信者Aは、$0<x_A<p_1-1$なる整数x_Aをランダムに選び、
【数6】$y_A=\exp(a_1:x_A)\pmod{p_1}$，
を計算し、
受信者Bは、$0<x_B<p_1-1$なる整数x_Bをランダムに選び、
【数7】$y_B=\exp(a_1:x_B)\pmod{p_1}$，
を計算し（ただし、exp（a：x）はaをx乗した値を表わす。）、
センタへの登録処理として、送信者Aおよび受信者Bは、自分のＩＤ情報をセンタに登録し、センタは送信者AのＩＤ情報I_Aから、$I_A+i_A\pmod{p_2-1}$が平方剰余、かつ、$I_A\neq I_B$ならば$I_A+i_A\pmod{p_2-1}$

4

$\neq I_B+i_B\pmod{p_2-1}$となるように正整数i_Aを選び、送信者Aに固有の秘密鍵s_Aを、
【数8】$s_A=\exp(I_A+i_A:1/2)\pmod{p_2-1}$，
にて計算し、同様に受信者BのＩＤ情報I_Bから、送信者Bに固有の秘密鍵s_Bを、
【数9】$s_B=\exp(I_B+i_B:1/2)\pmod{p_2-1}$，
にて計算し、各々を送信者Aおよび受信者Bに安全に配布し、このとき、ＩＤ情報が異なれば対応する秘密鍵も異なり、送信者Aはy_Aと、秘密鍵s_Aに対応する公開鍵
【数10】$v_A=\exp(a_2:s_A)\pmod{p_2}$，
との組（y_A，v_A）を送信者Aの公開鍵として登録し、受信者Bはy_Bと、秘密鍵s_Bに対応する公開鍵
【数11】$v_B=\exp(a_2:s_B)\pmod{p_2}$，
との組（y_B，v_B）を受信者Bの公開鍵として登録し、
マスタ鍵共有処理として、送信者Aは、受信者Bとの間で共通に保有する関数gを用いて、自分の秘密鍵である（x_A，s_A）と受信者Bの公開鍵である（y_B，v_B）から、マスタ鍵$K_{A.B}$を、
【数12】$K_{A.B}=g(\exp(y_B:x_A)\pmod{p_1},\ \exp(v_B:s_A)\pmod{p_2})$，
にて作成し、受信者Bは、自分の秘密鍵である（x_B，s_B）と送信者Aの公開鍵である（y_A，v_A）を用いて、マスタ鍵$K_{B.A}$を、
【数13】$K_{B.A}=g(\exp(y_A:x_B)\pmod{p_1},\ \exp(v_A:s_B)\pmod{p_2})$，
にて作成し、
このとき、$K_{A.B}=K_{B.A}$が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合S_A、または、送信者Aの秘密鍵（x_A，s_A）と鍵生成関数θから、
【数14】$K(A)=\theta(x_A,s_A)$，
にて作成した鍵K（A）を用いてマスタ鍵の集合S_Aを暗号化した
【数15】$C(A)=E_A(K(A);S_A)$，
を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、$E_A(k;M)$はAが所持する秘密鍵暗号アルゴリズムにより平文Mを鍵kにて暗号化した結果を表わす。）、
メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E（k；

5

P）と、データ暗号化鍵kをマスタ鍵$K_{A,B}$にて暗号化した暗号文E（$K_{A,B}$；k）をメール受信者Bに送信し、受信者Bは、マスタ鍵$K_{B,A}$を用いてE（$K_{A,B}$；k）からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE（k；P）からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項5】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理として、センタは、素数p_1と、p_2-1が二つの大きな素数を因数として持つ素数p_2と、整数a_1，a_2を公開し、p_2-1の素因数分解を秘密とし、送信者Aは、$0<x_A<p_1-1$なる整数x_Aをランダムに選び、

【数16】$y_A=\exp(a_1 : x_A) \pmod{p_1}$，

を計算し、受信者Bは、$0<x_B<p_1-1$なる整数x_Bをランダムに選び、

【数17】$y_B=\exp(a_1 : x_B) \pmod{p_1}$，

を計算し、センタへの登録処理として、送信者Aおよび受信者Bは、自分のＩＤ情報をセンタに登録し、センタは送信者AのＩＤ情報I_Aから、送信者Aに固有の秘密鍵s_Aを正数eを用いて、

【数18】$s_A=\exp(I_A : e) \pmod{p_2-1}$，

にて計算し、同様に受信者BのＩＤ情報I_Bから、送信者Bに固有の秘密鍵s_Bを正数eを用いて、

【数19】$s_B=\exp(I_B : e) \pmod{p_2-1}$，

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し（ただし、exp（a：x）はaをx乗した値を表わす）、

このとき、ＩＤ情報が異なれば対応する秘密鍵も異なり、送信者Aはy_Aと、秘密鍵s_Aに対応する公開鍵

【数20】$v_A=\exp(a_2 : s_A) \pmod{p_2}$，

の組（y_A，v_A）を送信者Aの公開鍵として登録し、受信者Bはy_Bと、秘密鍵s_Bに対応する公開鍵

【数21】$v_B=\exp(a_2 : s_B) \pmod{p_2}$，

の組（y_B，v_B）を受信者Bの公開鍵として登録し、マスタ鍵の共有処理として、送信者Aは、受信者Bとの間で共通に保有する関数gを用いて、自分の秘密鍵である（x_A，s_A）と受信者Bの公開鍵である（y_B，v_B）から、マスタ鍵$K_{A,B}$を、

【数22】$K_{A,B}=g(\exp(y_B : x_A) \pmod{p_1}, \exp(v_B : s_A) \pmod{p_2})$，

にて作成し、受信者Bは、自分の秘密鍵である（x_B，s_B）と送信者Aの公開鍵である（y_A，v_A）を用いて、マスタ鍵$K_{B,A}$を、

【数23】$K_{B,A}=g(\exp(y_A : x_B) \pmod{p_1}, \exp(v_A : s_B) \pmod{p_2})$，

にて作成し、このとき、$K_{A,B}=K_{B,A}$が成立し、

特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ

6

鍵からなる集合S_A、または、送信者Aの秘密鍵（x_A，s_A）と鍵生成関数θから、

【数24】$K(A)=\theta(x_A, s_A)$，

にて作成した鍵K（A）を用いてマスタ鍵の集合S_Aを暗号化した

【数25】$C(A)=E_A(K(A) ; S_A)$，

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、E_A（k；M）はAが所持する秘密鍵暗号アルゴリズムにより平文Mを鍵kにて暗号化した結果を表わす）、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E（k；P）と、データ暗号化鍵kをマスタ鍵$K_{A,B}$にて暗号化した暗号文E（$K_{A,B}$；k）をメール受信者Bに送信し、受信者Bは、マスタ鍵$K_{B,A}$を用いてE（$K_{A,B}$；k）からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE（k；P）からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項6】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、センタは、素数pと合成数$n=p_1 \cdot p_2$と整数aを公開し、nの素因数分解と正数αを秘密とし、送信者Aは、$0<x_A<p-1$なる整数x_Aをランダムに選び、

【数26】$y_A=\exp(a : x_A) \pmod{p}$，

を計算し、受信者Bは、$0<x_B<p-1$なる整数x_Bをランダムに選び、

【数27】$y_B=\exp(a : x_B) \pmod{p}$，

を計算し、センタへの登録処理として、送信者Aおよび受信者Bは、自分のＩＤ情報をセンタに登録し、センタは送信者AのＩＤ情報I_Aから、$I_A+i_A \pmod{l.c.d(p_1-1, p_2-1)}$が平方剰余、かつ、$I_A \neq I_B$ならば$I_A+i_A \pmod{l.c.d(p_1-1, p_2-1)} \neq I_B+i_B \pmod{l.c.d(p_1-1, p_2-1)}$となるように正整数$i_A$を選び、送信者Aに固有の鍵（$s_A$，$v_A$）を、

【数28】$s_A=\exp(I_A+i_A : 1/2) \pmod{l.c.d(p_1-1, p_2-1)}$，

$v_A=\exp(\alpha : s_A) \pmod{n}$，

にて計算し、同様に受信者BのＩＤ情報I_Bから、受信者Bに固有の鍵（s_B，v_B）を、

【数29】$s_B=\exp(I_B+i_B : 1/2) \pmod{l.c.d(p_1-1, p_2-1)}$，

$v_B=\exp(\alpha : s_B) \pmod{n}$，

にて計算し、各々を送信者Aおよび受信者Bに安全に配

7

布し（ただし、exp(a：x）はaをx乗した値を表わす）、
このとき、ＩＤ情報が異なれば対応する鍵も異なり、送信者Ａは(y_A, v_A)を送信者Ａの公開鍵として登録し、受信者Ｂは（y_B, v_B）を受信者Ｂの公開鍵として登録し、マスタ鍵共有処理として、
送信者Ａは、受信者Ｂとの間で共通に保有する関数ｇを用いて、自分の秘密鍵である（x_A, s_A）と受信者Ｂの公開鍵である（y_B, v_B）から、マスタ鍵$K_{A,B}$を、
【数30】$K_{A,B}=g(\exp(y_B:x_A)\pmod p), \exp(v_B:s_A)\pmod n)$,
にて作成し、受信者Ｂは、自分の秘密鍵である（x_B, s_B）と送信者Ａの公開鍵である（y_A, v_A）を用いてマスタ鍵$K_{B,A}$を、
【数31】$K_{B,A}=g(\exp(y_A:x_B)\pmod p), \exp(v_A:s_B)\pmod n)$,
にて作成し、このとき、$K_{A,B}=K_{B,A}$が成立し、特に、送信者Ａは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者Ａ間の各マスタ鍵からなる集合S_A、または、送信者Ａの秘密鍵（x_A, s_A）と鍵生成関数θから、
【数32】$K(A)=\theta(x_A, s_A)$,
にて作成した鍵Ｋ(Ａ）を用いてマスタ鍵の集合S_Aを暗号化した
【数33】$C(A)=E_A(K(A):S_A)$,
を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、E_A(ｋ；Ｍ）はＡが所持する秘密鍵暗号アルゴリズムにより平文Ｍを鍵ｋにて暗号化した結果を表わす）、
メール本文の暗復号化処理として、送信者Ａは、データ暗号化鍵ｋをランダムに選び、受信者Ｂとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Ｐをデータ暗号化鍵ｋにて暗号化した暗号文Ｅ(ｋ；Ｐ）と、データ暗号化鍵ｋをマスタ鍵$K_{A,B}$にて暗号化した暗号文Ｅ($K_{A,B}$；ｋ）をメール受信者Ｂに送信し、受信者Ｂは、マスタ鍵$K_{B,A}$を用いてＥ($K_{A,B}$；ｋ）からデータ暗号化鍵ｋを復号化し、さらにデータ暗号化鍵ｋを用いてＥ(ｋ；Ｐ）からメール本文Ｐを復号化することを特徴とする電子メール暗号化方法。
【請求項７】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Ａが受信者Ｂに対して送信するメール文を暗号化する電子メール暗号化方法であって、
準備処理として、センタは、素数ｐと合成数$n=p_1\cdot p_2$と整数ａを公開し、ｎの素因数分解と正数αを秘密とし、送信者Ａは、$0<x_A<p-1$なる整数x_Aをランダムに選び、

8

【数34】$y_A=\exp(a:x_A)\pmod p$,
を計算し、受信者Ｂは、$0<x_B<p-1$なる整数x_Bをランダムに選び、
【数35】$y_B=\exp(a:x_B)\pmod p$,
を計算し、センタへの登録処理として、送信者Ａおよび受信者Ｂは、自分のＩＤ情報をセンタに登録し、センタは送信者ＡのＩＤ情報I_Aから、送信者Ａに固有の鍵（s_A, v_A）を正数ｅを用いて、
【数36】$s_A=\exp(I_A:e)\pmod{l.c.d(p_1-1, p_2-1)}$,
$v_A=\exp(\alpha:s_A)\pmod n$,
にて計算し、同様に受信者ＢのＩＤ情報I_Bから、受信者Ｂに固有の鍵（s_B, v_B）を、
【数37】$s_B=\exp(I_B:e)\pmod{l.c.d(p_1-1, p_2-1)}$,
$v_B=\exp(\alpha:s_B)\pmod n$,
にて計算し、各々を送信者Ａおよび受信者Ｂに安全に配布し（ただし、exp(a：x）はａをｘ乗した値を表わす）、このとき、ＩＤ情報が異なれば対応する秘密鍵も異なり、送信者Ａは（y_A, v_A）を送信者Ａの公開鍵として登録し、受信者Ｂは（y_B, v_B）を受信者Ｂの公開鍵として登録し、マスタ鍵共有処理として、送信者Ａは、受信者Ｂとの間で共通に保有する関数ｇを用いて、自分の秘密鍵である（x_A, s_A）と受信者Ｂの公開鍵である（y_B, v_B）から、マスタ鍵$K_{A,B}$を、
【数38】$K_{A,B}=g(\exp(y_B:x_A)\pmod p), \exp(v_B:s_A)\pmod n)$,
にて作成し、受信者Ｂは、自分の秘密鍵である（x_B, s_B）と送信者Ａの公開鍵である（y_A, v_A）を用いてマスタ鍵$K_{B,A}$を、
【数39】$K_{B,A}=g(\exp(y_A:x_B)\pmod p), \exp(v_A:s_B)\pmod n)$,
にて作成し、このとき、$K_{A,B}=K_{B,A}$が成立し、特に、送信者Ａは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者Ａ間の各マスタ鍵からなる集合S_A、または、送信者Ａの秘密鍵（x_A, s_A）と鍵生成関数θから、
【数40】$K(A)=\theta(x_A, s_A)$,
にて作成した鍵Ｋ(Ａ）を用いてマスタ鍵の集合S_Aを暗号化した
【数41】$C(A)=E_A(K(A):S_A)$,
を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、E_A(ｋ；Ｍ）はＡが所持する秘密鍵暗号アルゴリズムにより平文Ｍを鍵ｋにて暗号化した結果を表わす）、
メール本文の暗復号化処理として、送信者Ａは、データ暗号化鍵ｋをランダムに選び、受信者Ｂとの間で共通に

9

保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E(k；P)と、データ暗号化鍵kをマスタ鍵$K_{A,B}$にて暗号化した暗号文E($K_{A,B}$；k)をメール受信者Bに送信し、受信者Bは、マスタ鍵$K_{B,A}$を用いてE($K_{A,B}$；k)からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE(k；P)からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項8】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、

準備処理として、センタは、素数p_1，p_2と整数a_1，a_2を公開し、剰余環$Z/(p_2-1)$の元を出力する秘密鍵暗号アルゴリズムおよび鍵rを秘密情報とし（センタの秘密情報である秘密鍵暗号アルゴリズムにより、平文Mを鍵kで暗号化した結果をE_0(k；M)で表わす）、

送信者Aは、$0<x_A<p_1-1$なる整数x_Aをランダムに選び、

【数42】$y_A=\exp(a_1 : x_A) \pmod{p_1}$，

を計算し、受信者Bは、$0<x_B<p_1-1$なる整数x_Bをランダムに選び、

【数43】$y_B=\exp(a_1 : x_B) \pmod{p_1}$，

を計算し（ただし、exp(a：x)はaをx乗した値を表わす）、

センタへの登録処理として、送信者Aおよび受信者Bは、自分のＩＤ情報をセンタに登録し、センタは送信者AのＩＤ情報I_Aから送信者Aに固有の秘密鍵s_Aを、

【数44】$s_A=E_0(r ; I_A)$，

にて計算し、同様に受信者BのＩＤ情報I_Bから、送信者Bに固有の秘密鍵s_Bを、

【数45】$s_B=E_0(r ; I_B)$，

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し、このとき、ＩＤ情報が異なれば対応する秘密鍵も異なり、送信者Aは、y_Aと、秘密鍵s_Aに対応する公開鍵

【数46】$v_A=\exp(a_2 : s_A) \pmod{p_2}$，

の組(y_A，v_A)を送信者Aの公開鍵として登録し、受信者Bは、y_Bと、秘密鍵s_Bに対応する公開鍵

【数47】$v_B=\exp(a_2 : s_B) \pmod{p_2}$，

の組(y_B，v_B)を受信者Bの公開鍵として登録し、マスタ鍵の共有処理として、

送信者Aは、受信者Bとの間で共通に保有する関数gを用いて、自分の秘密鍵である(x_A，s_A)と受信者Bの公開鍵である(y_B，v_B)から、マスタ鍵$K_{A,B}$を、

【数48】$K_{A,B}=g(\exp(y_B : x_A) \pmod{p_1}, \exp(v_B : s_A) \pmod{p_2})$，

にて作成し、受信者Bは、自分の秘密鍵である(x_B，s_B)と送信者Aの公開鍵である(y_A，v_A)を用いて、マスタ鍵$K_{B,A}$を、

10

【数49】$K_{B,A}=g(\exp(y_A : x_B) \pmod{p_1}, \exp(v_A : s_B) \pmod{p_2})$，

にて作成し、このとき、$K_{A,B}=K_{B,A}$が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合S_A、または、送信者Aの秘密鍵(x_A，s_A)と鍵生成関数θから、

【数50】$K(A)=\theta(x_A, s_A)$，

にて作成した鍵K(A)を用いてマスタ鍵の集合S_Aを暗号化した

【数51】$C(A)=E_A(K(A) ; S_A)$，

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、E_A(k；M)はAが所持する秘密鍵暗号アルゴリズムにより平文Mを鍵kにて暗号化した結果を表わす）、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E(k；P)と、データ暗号化鍵kをマスタ鍵$K_{A,B}$にて暗号化した暗号文E($K_{A,B}$；k)をメール受信者Bに送信し、受信者Bは、マスタ鍵$K_{B,A}$を用いてE($K_{A,B}$；k)からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE(k；P)からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項9】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、準備処理として、センタは、素数pと合成数$n=p_1 \cdot p_2$と整数aを公開し、整数αおよび剰余環Z/(N)の元を出力する秘密鍵暗号アルゴリズムおよび鍵rを秘密情報とし（ただし、$N=l.c.d(p_1-1, p_2-1)$であり、センタの秘密情報である秘密鍵暗号アルゴリズムにより平文Mを鍵kで暗号化した結果をE_0(k；M)で表わす）、

送信者Aは、$0<x_A<p-1$なる整数x_Aをランダムに選び、

【数52】$y_A=\exp(a : x_A) \pmod{p}$，

を計算し、受信者Bは、$0<x_B<p_1-1$なる整数x_Bをランダムに選び、

【数53】$y_B=\exp(a : x_B) \pmod{p}$，

を計算し、センタへの登録処理として、送信者Aおよび受信者Bは、自分のＩＤ情報をセンタに登録し、センタは送信者AのＩＤ情報I_Aから送信者Aに固有の鍵(s_A，v_A)を、

【数54】$s_A=E_0(r ; I_A)$，

$v_A=\exp(\alpha : s_A) \pmod{n}$，

11

にて計算し、同様に受信者BのＩＤ情報I_Bから受信者Bに固有の鍵(s_B, v_B)を、

【数55】$s_B = E_0(r ; I_B)$,

$v_B = \exp(\alpha : s_B) \pmod n$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配布し、このとき、ＩＤ情報が異なれば対応する鍵も異なり、送信者Aは(y_A, v_A)を送信者Aの公開鍵として登録し、受信者Bは(y_B, v_B)を受信者Bの公開鍵として登録し、マスタ鍵共有処理として、

送信者Aは、受信者Bとの間で共通に保有する関数gを用いて、自分の秘密鍵である(x_A, s_A)と受信者Bの公開鍵である(y_B, v_B)から、マスタ鍵$K_{A.B}$を、

【数56】$K_{A.B} = g(\exp(y_B : x_A) \pmod p, \exp(v_B : s_A) \pmod n)$,

にて作成し、受信者Bは、自分の秘密鍵である(x_B, s_B)と送信者Aの公開鍵である(y_A, v_A)を用いてマスタ鍵$K_{B.A}$を、

【数57】$K_{B.A} = g(\exp(y_A : x_B) \pmod p, \exp(v_A : s_B) \pmod n)$,

にて作成し、このとき、$K_{A.B} = K_{B.A}$が成立し、特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合S_A、または、送信者Aの秘密鍵(x_A, s_A)と鍵生成関数θから、

【数58】$K(A) = \theta(x_A, s_A)$,

にて作成した鍵K(A)を用いてマスタ鍵の集合S_Aを暗号化した

【数59】$C(A) = E_A(K(A) ; S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使うこととし（ただし、$E_A(k ; M)$はAが所持する秘密鍵暗号アルゴリズムにより平文Mを鍵kにて暗号化した結果を表わす）、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E(k；P)と、データ暗号化鍵kをマスタ鍵$K_{A.B}$にて暗号化した暗号文$E(K_{A.B} ; k)$をメール受信者Bに送信し、受信者Bは、マスタ鍵$K_{B.A}$を用いて$E(K_{A.B} ; k)$からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE(k；P)からメール本文Pを復号化することを特徴とする電子メール暗号化方法。

【請求項１０】請求項４、５、６、７、８または９において、

マスタ鍵共有処理の中で、送信者Aと受信者Bとの間で共通に保有する関数gとして、

【数60】$g(x_1, x_2) = h(\phi(x_1, x_2))$,

12

なる関数を用いて（ただし、hはハッシュ関数、φは、

【数61】$\phi : Z/(p) \times Z/(n) \rightarrow Z/(pn)$

$((x, x) \rightarrow x)$,

なる同型写像を表わし、Z/(m)は整数mを法とする剰余環を表わし、xはそれぞれの剰余環においてxを代表元とする剰余類を表わす。）、マスタ鍵を作成する電子メール暗号化方法。

【請求項１１】請求項４、５、６、７、８または９において、マスタ鍵共有処理の中で、送信者Aと受信者Bとの間で共通に保有する関数gとして、

【数62】$g(x_1, x_2) = h(x_1 * x_2)$,

なる関数を用いて（ただし、hはハッシュ関数、$x_1 * x_2$はx_1とx_2の排他的論理和を表わす）、マスタ鍵を作成する電子メール暗号化方法。

【請求項１２】請求項３、４、５、６、７、８、９または１１において、

メール本文の暗復号化処理として、送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E(k；P)と、データ暗号化鍵kとマスタ鍵$K_{A.B}$の排他的論理和$k * K_{A.B}$を受信者Bに送信し、受信者Bは、マスタ鍵$K_{B.A}$と$k * K_{A.B}$の排他的論理和を取ることにより、データ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE(k；P)からメール本文Pを復号化する電子メール暗号化システム。

【請求項１３】通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、送信者Aが受信者Bに対して送信するメール文を暗号化する電子メール暗号化方法であって、送信者および受信者はそれぞれの秘密鍵を内蔵した演算機能付き記憶媒体を所持し、送信者は通信ネットワークに接続された計算機１と送信者の記憶媒体Ａを用いて、請求項１から請求項１２の電子メール暗号化方法に従い、暗号化処理を記憶媒体Ａ内で行ない、送信文を計算機１に出力し、計算機１から通信回線を介して受信者の使用する計算機２に送信し、受信者は、送信者から送られてきた送信文を計算機２から受信者の演算機能付き記憶媒体Ｂに出力し、記憶媒体Ｂ内でデータ暗号化鍵およびメール本文を復号化することを特徴とする電子メール暗号化方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、通信ネットワークを介して文書を送受信する電子メール通信システムにおいて、ネットワーク上での盗聴や不正者によるなりすましに対して安全性を向上させた電子メール暗号化方法に関する。

【０００２】

【従来の技術】Internetにおける電子メールのセキュリティを強化することを目的として、文献「Linn, J., et

13

al., "Privacy Enhancement for Internet Electronic Mail:Part I, II, III, IV", RFC-1421-1424, 1993」に記載のＰＥＭ（Privacy Enhanced Mail）が提案されている。以下、ＰＥＭの電子メール暗号化技法について簡単に説明する。

【０００３】ＰＥＭでは、鍵管理に公開鍵暗号ＲＳＡ（参考文献「R.L.Rivest, A.Shamir, L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", Communications of the ACM, Vol.21, 1978」）を利用し、データの暗号化に米国暗号標準である秘密鍵暗号ＤＥＳ（参考文献「Data EncryptionStandard, FIPS-PUB-46, 1977」）を用いている。

【０００４】送信者Ａは受信者Ｂにネットワークを介して電子メールを送る。

【０００５】Step 1．Ａはデータ暗号化鍵Ｋをランダムに作り、鍵Ｋを用いてメール本文ＰをＤＥＳにより暗号化する。すなわち、メール本文Ｐの暗号文C_1を、

【０００６】

【数63】$C_1 = E(K : P)$，

とする。

【０００７】Step 2．ＡはＢの公開鍵（e_B, n_B）を用いて鍵ＫをＲＳＡにより暗号化する。　すなわち、鍵Ｋの暗号文C_2を、

【０００８】

【数64】$C_2 = \exp(K : e_B) \pmod{n_B}$，

とする。ただし、exp(a：x)はａをｘ乗した値を表わす。

【０００９】Step 3．Ａはメール本文Ｐを公開情報であるハッシュ関数ｆを用いて圧縮し、Ａの秘密鍵d_Aと公開鍵n_Aを用いてｆ(Ｐ)にＲＳＡ署名を行なう。すなわち、ｆ(Ｐ)に対する署名文$sgn_A(P)$を、

【００１０】

【数65】$sgn_A(P) = \exp(f(P) : d_A) \pmod{n_A}$，

とする。

【００１１】Step 4．ＡはC_1, C_2, $sgn_A(P)$をＢに送る。

【００１２】Step 5．Ｂは自分の秘密鍵d_Bを用いて、C_2から、

【００１３】

【数66】$K = \exp(C_2 : d_B) \pmod{n_B}$，

により、データ暗号化鍵Ｋを復号化する。

【００１４】Step 6．Ｂは鍵Ｋを用いて、

【００１５】

【数67】$P = D(K ; C_1)$，

により、メール本文Ｐを復号化する。

【００１６】Step 7．Ｂはメール本文ＰがＡから送られてきたことを確めるため、ハッシュ関数ｆとＡの公開鍵（e_A, n_A）を用いて、

【００１７】

【数68】$f(P) = \exp(sgn_A(P) : e_A) \pmod{n_A}$，

14

を確認する。

【００１８】ＰＥＭには次の問題点が考えられる。

【００１９】（１）安全性の立場から、データ暗号化鍵は頻繁に変更することが望ましい。ＰＥＭの場合、電子メール通信をする機会が多い相手であっても、データ暗号化鍵を変更する度に相手の公開鍵を用いてＲＳＡ暗号により新しいデータ暗号化鍵を暗号化して送らなければならない。特に、一度に多数の相手にメールを送信したい場合、ＲＳＡ暗号は暗号化のための計算量が比較的大きいため、データ暗号化鍵の暗号化のための計算処理負担が大きい。

【００２０】（２）ＲＳＡ暗号を用いた鍵配送では、鍵の復号化は受信者の秘密鍵のみで行なわれるため認証機能はない。そのため、ＰＥＭでは、ＲＳＡを用いたディジタル署名を付加することで認証機能を実現している。しかし、ディジタル署名は作成と検証のための計算処理負担が大きく、さらに、メール暗号文に付加するヘッダ情報が大きくなる欠点を持つ。

【００２１】（３）ＰＥＭにおいては、ネットワークの各利用者の鍵は利用者自身が作成するため、偶然にも異なる利用者の鍵が一致してしまう可能性がある。たとえば、利用者Ａと利用者Ｂの鍵が一致していることに、ＡがＢの公開鍵から気が付くと、ＡはＢになりすましたり、Ｂと他の利用者の電子メール通信を盗聴することができる。

【００２２】

【発明が解決しようとする課題】本発明の目的は、通信ネットワーク上でメールの送受信を行なう電子メール通信システムにおいて、メールシステムや機種に特定しないで通常のメールと併用できる特徴を有し、かつ、電子メールの送信者および受信者双方におけるセキュリティ機能実現のための計算処理およびメモリ負担が少なく、かつ、利用者の鍵の一致の心配がない盗聴や不正者のなりすましに対して安全性の高い電子メール暗号化方法を提案することにある。

【００２３】

【課題を解決するための手段】本発明は、通信ネットワーク上でデータの送受信を行なう電子メール通信システムにおいて、高効率・高安全な電子メール暗号化方法を提案するものである。

【００２４】具体的実現方法の１つとしては、送信者Ａが受信者Ｂに対して送信するメール文を暗号化する電子メール暗号化方法であって、

①準備処理

センタは、素数ｐと合成数$n = p_1 \cdot p_2$と整数ａを公開し、ｎの素因数分解と正数αを秘密とする。

【００２５】送信者Ａは、$0 < x_A < p-1$なる整数x_Aをランダムに選び、

【００２６】

【数69】$y_A = \exp(a : x_A) \pmod{p}$，

を計算し、受信者Bは、$0<x_B<p-1$なる整数x_Bをランダムに選び、

【0027】

【数70】$y_B=\exp(a:x_B)\pmod p$,

を計算する。ただし、$\exp(a:x)$はaをx乗した値を表わす。

【0028】②センタへの登録処理

送信者Aおよび受信者Bは、自分のID情報をセンタに登録し、センタは送信者AのID情報I_Aから、送信者Aに固有の鍵（s_A, v_A）を正数eを用いて、

【0029】

【数71】$s_A=\exp(I_A:e)\pmod{l.c.d(p_1-1,\ p_2-1)}$,

$v_A=\exp(\alpha:s_A)\pmod n$,

にて計算し、同様に受信者BのID情報I_Bから、受信者Bに固有の鍵（s_B, v_B）を、

【0030】

【数72】$s_B=\exp(I_B:e)\pmod{l.c.d(p_1-1,\ p_2-1)}$,

$v_B=\exp(\alpha:s_B)\pmod n$,

にて計算し、各々を送信者Aおよび受信者Bに安全に配布する。ただし、l．c．d（x，y）は整数x，yの最小公倍数を表わす。

【0031】このとき、ID情報が異なれば対応する秘密鍵も異なる。

【0032】送信者Aは（y_A, v_A）を送信者Aの公開鍵として登録し、受信者Bは（y_B, v_B）を受信者Bの公開鍵として登録する。

【0033】③マスタ鍵共有処理

送信者Aは、受信者Bとの間で共通に保有する関数gを用いて、自分の秘密鍵である（x_A, s_A）と受信者Bの公開鍵である（y_B, v_B）から、マスタ鍵$K_{A.B}$を、

【0034】

【数73】$K_{A.B}=g(\exp(y_B:x_A)\pmod p,\ \exp(v_B:s_A)\pmod n)$,

にて作成し、受信者Bは、自分の秘密鍵である（x_B, s_B）と送信者Aの公開鍵である（y_A, v_A）を用いてマスタ鍵$K_{B.A}$を、

【0035】

【数74】$K_{B.A}=g(\exp(y_A:x_B)\pmod p,\ \exp(v_A:s_B)\pmod n)$,

にて作成する。

【0036】このとき、$K_{A.B}=K_{B.A}$が成立する。

【0037】特に、送信者Aは電子メールを送信する機会が多い受信者に対しては、それらの受信者と送信者A間の各マスタ鍵からなる集合S_A、または、送信者Aの秘密鍵（x_A, s_A）と鍵生成関数θから、

【0038】

【数75】$K(A)=\theta(x_A,\ s_A)$,

にて作成した鍵K(A)を用いてマスタ鍵の集合S_Aを暗

号化した

【0039】

【数76】$C(A)=E_A(K(A):S_A)$,

を記憶し、以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに相手の公開鍵と自分の秘密鍵からマスタ鍵を作成することなく、記憶されているマスタ鍵を使う。ただし、$E_A(k:M)$はAが所持する秘密鍵暗号アルゴリズムにより平文Mを鍵kにて暗号化した結果を表わす。

【0040】④メール本文の暗復号化処理

送信者Aは、データ暗号化鍵kをランダムに選び、受信者Bとの間で共通に保有する秘密鍵暗号系アルゴリズムを用いて、メール本文Pをデータ暗号化鍵kにて暗号化した暗号文E（k：P）と、データ暗号化鍵kをマスタ鍵$K_{A.B}$にて暗号化した暗号文$E(K_{A.B}:k)$をメール受信者Bに送信する。

【0041】受信者Bは、マスタ鍵$K_{B.A}$を用いて$E(K_{A.B}:k)$からデータ暗号化鍵kを復号化し、さらにデータ暗号化鍵kを用いてE（k：P）からメール本文Pを復号化する。

【0042】

【作用】本発明における電子メール暗号化方法では、電子メールの送信者および受信者はそれぞれ自分の秘密鍵と相手の公開鍵からマスタ鍵の共有を行ない、秘密鍵暗号を用いてメール本文の暗号化およびデータ暗号化鍵の配送を行なうことにより、セキュリティ機能実現のための送受信者双方の計算処理負担を削減し、かつ、ディジタル署名などの付加情報を付けることなく送信者の認証を実現した。特に、頻繁にメール通信を行なう相手については鍵情報としてマスタ鍵のみを記憶しておけば、受信者の公開鍵の必要もなく、かつ、データ暗号化鍵の更新の度にマスタ鍵の生成を行なう必要もなく、高速な暗号化処理が可能となった。

【0043】また、ID情報は利用者（電子メールの送信者および受信者）毎に異なることを利用して、センタと利用者が協力して利用者の鍵生成を行なうことで、利用者の鍵が一致することがなく、盗聴や不正者のなりすましに対して高い安全性を実現した。

【0044】

【実施例】以下、図面を用いて、本発明の実施例について詳しく説明する。

【0045】図1は、本発明の実施例のシステム構成を示す図である。同図のシステムは、複数の利用者側装置100とセンタ側装置200とから構成されている。利用者側装置100は互いに通信回線300を介して接続されている。

【0046】図2は、本発明における電子メール暗号化方法の概念図を示す。

【0047】図3は、実施例1から9における利用者側装置100の内部構成を示す。利用者側装置100は、乱数発

17

生器101、べき乗算器102、鍵生成器103、演算器104、暗復号化装置105、ハッシュ計算器106、メモリ107、通信装置108を備えている。

【００４８】図４は、センタ側装置200の内部構成を示す。センタ側装置200は、素数発生器201、原始根生成器202、秘密鍵作成装置203、演算器204を備えている。

【００４９】図５は、カード400の内部構成を示す。カード400は、乱数発生器401、べき乗算器402、鍵生成器403、演算器404、暗復号化装置405、ハッシュ計算器406、メモリ407、出力装置408を備えている。

【００５０】図６は、実施例１０における利用者側装置500の内部構成を示す。利用者側装置500は、カード読取装置501、通信装置502を備えている。

【００５１】ネットワークの利用者は通信回線に接続された自分の利用者側装置100（カード400と利用者側装置500）を用いて他の利用者側装置100（カード400と利用者側装置500）を使用する別の利用者に対して電子メール通信を行なうケースを考える。

【００５２】このとき、電子メールの暗号化方法について＊

18

＊て以下の実施例において詳しく説明する。

【００５３】Ｚは整数環を表わし、Ｚ/(ｎ)は整数ｎを法とする剰余環を表わす。特に、ｎが素数のとき、Ｚ/(ｎ)は剰余体になる。ｘ∈Ｚに対して、ｘは対応する剰余環におけるｘを代表元とする剰余類を表わす。また、exp(ａ：ｘ)はａをｘ乗した値を表わす。

【００５４】ネットワークの利用者のＩＤ情報はすべてｔビット以下で表わされる場合、利用者のＩＤ情報はＺ/(exp(２：ｔ)－１)の元と考えることができる。このとき、利用者のＩＤ情報の集合Λを、Λ＝Ｚ/(exp(２：ｔ)－１)と定義する。

【００５５】（実施例１）

①準備

ネットワークの各利用者λはそれぞれ自身の利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の情報を作成し、公開鍵のみを公開・登録する。

【００５６】秘密鍵：

【００５７】

【数77】

$$\cdot x_{\lambda j} \in Z \ s.t \ 0 < x_{\lambda j} < p-1 \quad \text{for } j = 1, \cdots, n.$$

※【数78】

公開鍵：

【００５８】

※

$$\cdot y_{\lambda j} = \exp(a : x_{\lambda j}) \pmod p \quad \text{for } j = 1, \cdots, n.$$

ただし、ｐは素数、ａは０＜ａ＜ｐでＺ/(ｐ)の原始根となる整数、ｎはセキュリティパラメータを表わし、予め与えられているものとする。

【００５９】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置104があり、この秘密鍵暗号系アルゴリズムを用いて平文Ｍを鍵Ｋで暗号化した結果および復号化した結果をそれぞれＥ(Ｋ；Ｍ)，Ｄ(Ｋ；Ｍ)で表わす。

【００６０】②マスタ鍵の共有

ネットワークの利用者であるＡ，Ｂについて、ＡはＢに対して電子メールを送りたい。この目的の下で、Ａ，Ｂは次の手順を実行する。

【００６１】ＡはＡの利用者側装置100A内のべき乗算器102Aおよび演算器104Aを用いて自分の秘密鍵x_{Aj}とＢの公開鍵y_{Bj}（ｊ＝１，…，ｎ）からマスタ鍵$K_{A.B}$を、

【００６２】

【数79】$K_{A.B} = \Pi\{\exp(y_{Bj} : x_{Aj}) \pmod p \mid j = 1, \cdots, n\}$，

にて計算する。ただし、記号100A等については、数字の後のアルファベットにより利用者の識別を行なう。

【００６３】同様にして、ＢはＢの利用者側装置100B内のべき乗算器102Bおよび演算器104Bを用いて自分の秘密鍵x_{Bj}とＡの公開鍵y_{Aj}（ｊ＝１，…，ｎ）からマスタ鍵$K_{B.A}$を、

【００６４】

【数80】$K_{B.A} = \Pi\{\exp(y_{Aj} : x_{Bj}) \pmod p \mid j = 1, \cdots, n\}$，

にて作成する。このとき、明らかに、

【００６５】

【数81】$K_{A.B} = K_{B.A}$，

が成立する。

【００６６】さらに、Ａは電子メールを送信する機会が多い利用者に対しては、それらの利用者とＡ間の各マスタ鍵の集合S_A、または、Ａの秘密情報x_{Aj}（ｊ＝１，…，ｎ）から利用者側装置100A内の鍵生成器103Aにより鍵Ｋ(Ａ)を作成し、暗復号化装置105Aを用いて鍵Ｋ(Ａ)によりS_Aを暗号化した

【００６７】

【数82】Ｃ(Ａ)＝Ｅ(Ｋ(Ａ)；S_A)，

を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【００６８】③メール本文の暗号化

Ａは、利用者側装置100A内の乱数発生器101Aを用いて乱数ｒを選び、ｒを入力として鍵生成器103Aからデータ暗号化鍵ｋを作成する。メール本文Ｐを暗復号化装置105Aを用いてデータ暗号化鍵ｋにより暗号化した暗号文C_1を、

【００６９】

【数83】$C_1 = E(k ; P)$，

にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵kをマスタ鍵$K_{A,B}$で暗号化した暗号文C_2を、

【0070】

【数84】$C_2=E(K_{A,B};k)$，

にて作成する。

【0071】Aは、通信装置108Aを用いてC_1とC_2をBに送る。

【0072】④メール本文の復号化

Bは送られてきたC_1とC_2に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B,A}$より、

【0073】

【数85】$k=D(K_{B,A};C_2)$，

にてデータ暗号化鍵kを復号化し、次にデータ暗号化鍵kを用いて、

【0074】

【数86】$P=D(k;C_1)$，

にて、メール本文Pを復号化する。

【0075】（実施例2）実施例2では、センタの存在を仮定して利用者の鍵情報が偶然にも一致することのない高い安全性をもつ電子メール暗号化方法について述べる。

【0076】①準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0077】公開情報：

・p_1；素数，

・$p_2=2q_1q_2+1$；素数，

・$a_1\in Z$ s.t $0<a_1<p_1$、かつ、a_1は$Z/(p_1)$で原始根，

・$a_2\in Z$ s.t $0<a_2<p_2$、かつ、a_1は$Z/(p_1)$で原始根，

秘密情報：

・q_1，$q_2\in Z$；素数．

ネットワークの各利用者λは利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0078】秘密鍵：

【0079】

【数87】・$x_\lambda\in Z$ s.t $0<x_\lambda<p_1-1$．

公開鍵：

【0080】

【数88】・$y_\lambda=\exp(a_1:x_\lambda)\pmod{p_1}$．

②センタへの登録

ネットワークの利用者λはセンタに自分のID情報I_λ＊

＊を登録する。

【0081】センタは、センタ側装置200内の秘密鍵作成装置203を用いて、

【0082】

【数89】$ed\equiv 1\pmod{l.c.d(q_1-1,\ q_2-1)}$，

なるe，d∈Zを作成し、利用者λのID情報I_λに対して、

【0083】

【数90】$s_\lambda=\exp(I_\lambda:e)\pmod{p_2-1}$，

を計算して、s_λを利用者λに安全に配布する。

【0084】このとき、

【0085】

【数91】

$s_\lambda\neq s_\mu$ if $I_\lambda\neq I_\mu\in\Lambda=Z/(p_2-1)$，

が成立することに注意する。

【0086】③マスタ鍵の共有

ネットワークの利用者λは、ベクトル$(y_\lambda,\ v_\lambda)$をλの公開鍵として登録を行なう。ただし、

【0087】

【数92】$v_\lambda=\exp(a_2:s_\lambda)\pmod{p_2}$．

さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文Mを鍵Kで暗号化した結果および復号化した結果をそれぞれ$E(K;M)$，$D(K;M)$で表わす。

【0088】ネットワークの利用者A，Bについて、AはBに対して電子メールを送りたい。この目的の下で、A，Bは次の手順を実行する

Aは Aの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵$(x_A,\ s_A)$とBの公開鍵$(y_B,\ v_B)$からマスタ鍵$K_{A,B}$を、

【0089】

【数93】$K_{A,B}=g(\phi(\exp(y_B:x_A)(\mathrm{mod}\ p_1),\ \exp(v_B:s_A)(\mathrm{mod}\ p_2)))$，

にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、Bの秘密鍵$(x_B,\ s_B)$とAの公開鍵$(y_A,\ v_A)$からマスタ鍵$K_{B,A}$を、

【0090】

【数94】$K_{B,A}=g(\phi(\exp(y_A:x_B)\pmod{p_1},\ \exp(v_A:s_B)\pmod{p_2}))$，

にて計算する。ただし、gはハッシュ計算器内で用いられるハッシュ関数を表わし、φは，

【0091】

【数95】

$$\phi:Z/(p_1)\times Z/(p_2)\rightarrow Z/(n)\quad((x,\ x)\rightarrow x)$$

【0092】このとき、明らかに、$K_{A,B}=K_{B,A}$，が成立する。

【0093】さらに、Aは電子メールを送信する機会が

21

多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合S_A、または、Aの秘密情報x_Aから利用者側装置100A内の鍵生成器103Aにより鍵K(A)を作成し、暗復号化装置105Aを用いて鍵K(A)によりS_Aを暗号化したC(A)＝E(K(A)；S_A)，を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【００９４】⑤メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数rを選び、rを入力として鍵生成器103Aからデータ暗号化鍵kを作成する。メール本文Pを暗復号化装置105Aを用いてデータ暗号化鍵kにより暗号化した暗号文C_1を、C_1＝E(k；P)，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵kをマスタ鍵$K_{A,B}$で暗号化した暗号文C_2を、C_2＝E($K_{A,B}$；k)，にて作成する。

【００９５】Aは、通信装置108Aを用いてC_1とC_2をBに送る。

【００９６】④メール本文の復号化

Bは送られてきたC_1とC_2に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B,A}$より、k＝D($K_{B,A}$；C_2)，にてデータ暗号化鍵kを復号化し、次にデータ暗号化鍵kを用いて、P＝D(k；C_1)，にて、メール本文Pを復号化する。

【００９７】（実施例３）実施例３は、実施例２においてセンタが作成する利用者λのための情報(s_λ，v_λ)を実施例２とは異なる別の関数により作成する一例を与える。

【００９８】①準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。ただし、関数fは秘密鍵作成装置203内に格納されているものとする。

【００９９】公開情報：

・p_1；素数，

・$p_2=2q_1q_2+1$；素数，

・$a_1\in Z$ s.t $0<a_1<p_1$、かつ、a_1は$Z/(p_1)$で原始根，

・$a_2\in Z$ s.t $0<a_2<p_2$、かつ、a_1は$Z/(p_1)$で原始根，

秘密情報：

・q_1，$q_2\in Z$；素数．

ネットワークの各利用者λは利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【０１００】秘密鍵：

【０１０１】

22

【数96】・$x_\lambda\in Z$ s.t $0<x_\lambda<p_1-1$．

公開鍵：

【０１０２】

【数97】・$y_\lambda=\exp(a_1：x_\lambda)\pmod{p_1}$．

②センタへの登録

ネットワークの利用者λはセンタに自分のＩＤ情報I_λを登録する。

【０１０３】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、利用者λのＩＤ情報I_λに対して、

（１）$I_\lambda+i_\lambda \pmod{p_2-1}$は平方剰余，

（２）$I_\lambda+i_\lambda \pmod{p_2-1}\neq I_\mu+i_\mu \pmod{p_2-1}$ if $\lambda\neq\mu$，

となるように正整数i_λを選び、

【０１０４】

【数98】

$s_\lambda=\exp(I_\lambda+i_\lambda)：1/2)\pmod{p_2-1}$

を計算して、s_λを利用者λに安全に配布する。

【０１０５】このとき、明らかに、$s_\lambda\neq s_\mu$ if $\lambda\neq\mu$，が成立する。

【０１０６】③マスタ鍵の共有

ネットワークの利用者λは、ベクトル（y_λ，v_λ）をλの公開鍵として登録を行なう。ただし、$v_\lambda=\exp(a_2：s_\lambda)\pmod{p_2}$．さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文Mを鍵Kで暗号化した結果および復号化した結果をそれぞれE(K；M)，D(K；M)で表わす。

【０１０７】ネットワークの利用者A，Bについて、AはBに対して電子メールを送りたい。この目的の下で、A，Bは次の手順を実行する

Aは Aの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵（x_A，s_A）とBの公開鍵（y_B，v_B）からマスタ鍵$K_{A,B}$を、

【０１０８】

【数99】$K_{A,B}=g(\phi(\exp(y_B：x_A)\pmod{p_1}，\exp(v_B：s_A)\pmod{p_2}))$，

にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、Bの秘密鍵（x_B，s_B）とAの公開鍵（y_A，v_A）からマスタ鍵$K_{B,A}$を、

【０１０９】

【数100】$K_{B,A}=g(\phi(\exp(y_A：x_B)\pmod{p_1}，\exp(v_A：s_B)\pmod{p_2}))$，

にて計算する。ただし、gはハッシュ計算器内で用いられるハッシュ関数を表わし、φは，

【０１１０】

【数101】

23 24

$\phi : Z/(p_1) \times Z/(p_2) \rightarrow Z/(n)$ $((x, x) \rightarrow x)$,

なる同型写像を表わす（$n = p_1 p_2$）。ここで、xはそれぞれの剰余環におけるxを代表元とする剰余類を表わす。

【０１１１】このとき、明らかに、$K_{A,B} = K_{B,A}$，が成立する。

【０１１２】さらに、Aは電子メールを送信する機会が多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合S_A、または、Aの秘密情報x_Aから利用者側装置100A内の鍵生成器103Aにより鍵K（A）を作成し、暗復号化装置105Aを用いて鍵K（A）によりS_Aを暗号化したC（A）＝E（K（A）；S_A），を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【０１１３】⑤メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数rを選び、rを入力として鍵生成器103Aからデータ暗号化鍵kを作成する。メール本文Pを暗復号化装置105Aを用いてデータ暗号化鍵kにより暗号化した暗号文C_1を、$C_1 = E(k ; P)$，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵kをマスタ鍵$K_{A,B}$で暗号化した暗号文C_2を、$C_2 = E(K_{A,B} ; k)$，にて作成する。

【０１１４】Aは、通信装置108Aを用いてC_1とC_2をBに送る。

【０１１５】④メール本文の復号化

Bは送られてきたC_1とC_2に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B,A}$より、$k = D(K_{B,A} ; C_2)$，にてデータ暗号化鍵kを復号化し、次にデータ暗号化鍵kを用いて、$P = D(k ; C_1)$，にて、メール本文Pを復号化する。

【０１１６】（実施例４）実施例４は、実施例２，３においてセンタが作成する利用者λのための情報（s_λ，v_λ）を実施例２，３とは異なる別の関数により作成する一例を与える。

【０１１７】①準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【０１１８】公開情報：

・p_1；素数，

・p_2；素数，

・$a_1 \in Z$ s.t $0 < a_1 < p_1$、かつ、a_1はZ/(p_1）で原始根，

・$a_2 \in Z$ s.t $0 < a_2 < p_2$、かつ、a_1はZ/(p_1）で原始根，

秘密情報：

・Z/($p_2 - 1$）の元を出力する秘密鍵暗号アルゴリズムおよび鍵$r \in Z$.

センタの秘密情報である秘密鍵暗号アルゴリズムにより、平文Mを鍵kで暗号化および復号化した結果をそれぞれ$E_0(k ; M)$，$D_0(k ; M)$で表わす。

【０１１９】ネットワークの各利用者λは利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【０１２０】秘密鍵：

【０１２１】

【数102】・$x_\lambda \in Z$ s.t $0 < x_\lambda < p_1 - 1$.

公開鍵：

【０１２２】

【数103】・$y_\lambda = \exp(a_1 : x_\lambda) \pmod{p_1}$.

②センタへの登録

ネットワークの利用者λはセンタに自分のＩＤ情報I_λを登録する。

【０１２３】センタは、センタ側装置200内の秘密鍵作成装置203を用いて、利用者λのＩＤ情報I_λに対して、

【０１２４】

【数104】$s_\lambda = E_0(r ; I_\lambda) \in Z/(p_2 - 1)$，

を計算して、s_λを利用者λに安全に配布する。

【０１２５】このとき、

【０１２６】

【数105】

$s_\lambda \neq s_\mu$ if $I_\lambda \neq I_\mu \in \Lambda = Z/(p_2 - 1)$，

が成立することに注意する。

【０１２７】③マスタ鍵の共有

ネットワークの利用者λは、ベクトル（y_λ，v_λ）をλの公開鍵として登録を行なう。ただし、$v_\lambda = \exp(a_2 : s_\lambda) \pmod{p_2}$．さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文Mを鍵Kで暗号化した結果および復号化した結果をそれぞれE（K；M），D（K；M）で表わす。

【０１２８】ネットワークの利用者A，Bについて、AはBに対して電子メールを送りたい。この目的の下で、A，Bは次の手順を実行する

AはAの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵（x_A，s_A）とBの公開鍵（y_B，v_B）からマスタ鍵$K_{A,B}$を、

【０１２９】

【数106】$K_{A,B} = g(\phi(\exp(y_B : x_A) \pmod{p_1}, \exp(v_B : s_A) \pmod{p_2}))$

，にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、Bの秘密鍵（x_B，s_B）とAの公開鍵（y_A，

25

v_A）からマスタ鍵$K_{B.A}$を、

【0130】

【数107】$K_{B.A}=g(\phi(\exp(y_A:x_B)\pmod{p_1}, \exp(v_A:s_B)\pmod{p_2}))$,

$\phi: Z/(p_1)\times Z/(p_2)\rightarrow Z/(n)$

なる同型写像を表わす（$n=p_1p_2$）。ここで、xはそれぞれの剰余環におけるxを代表元とする剰余類を表わす。

【0132】このとき、明らかに、$K_{A.B}=K_{B.A}$，が成立する。

【0133】さらに、Aは電子メールを送信する機会が多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合S_A、または、Aの秘密情報x_Aから利用者側装置100A内の鍵生成器103Aにより鍵K(A)を作成し、暗復号化装置105Aを用いて鍵K(A)によりS_Aを暗号化した$C(A)=E(K(A);S_A)$，を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0134】④メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数rを選び、rを入力として鍵生成器103Aからデータ暗号化鍵kを作成する。メール本文Pを暗復号化装置105Aを用いてデータ暗号化鍵kにより暗号化した暗号文C_1を、$C_1=E(k;P)$，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵kをマスタ鍵$K_{A.B}$で暗号化した暗号文C_2を、$C_2=E(K_{A.B};k)$，にて作成する。

【0135】Aは、通信装置108Aを用いてC_1とC_2をBに送る。

【0136】⑤メール本文の復号化

Bは送られてきたC_1とC_2に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B.A}$より、$k=D(K_{B.A};C_2)$，にてデータ暗号化鍵kを復号化し、次にデータ暗号化鍵kを用いて、$P=D(k;C_1)$，にて、メール本文Pを復号化する。

【0137】（実施例5）実施例5は実施例2の拡張版であり、αの値を秘密にすることで安全性をさらに向上させている。

【0138】①準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0139】公開情報：

・p；素数，

・$n=q\cdot q'$，

・$a\in Z$ s.t $0<a<p$、かつ、aはZ/(p)で原始根，

秘密情報：

26

＊にて計算する。ただし、gはハッシュ計算器内で用いられるハッシュ関数を表わし、ϕは，

【0131】

【数108】＊

$((x, x')\rightarrow x)$，

・$q, q'\in Z$；素数 s.t $q-1=2\xi_1\xi_2$，$q'-1=2\eta_1\eta_2$（$\xi_1, \xi_2, \eta_1, \eta_2$；素数），

・$\alpha\in Z$ s.t αはZ/(q)，Z/(q')で原始根．

ネットワークの各利用者λは利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0140】秘密鍵：

【0141】

【数109】・$x_\lambda\in Z$ s.t $0<x_\lambda<p-1$．

公開鍵：

【0142】

【数110】・$y_\lambda=\exp(a:x_\lambda)\pmod{p}$．

②センタへの登録

ネットワークの利用者λはセンタに自分のID情報I_λを登録する。

【0143】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、$ed\equiv 1\pmod{M}$，なるe，dを作成し、利用者λのID情報I_λに対して、$s_\lambda=\exp(I_\lambda:e)\pmod{N}$，

【0144】

【数111】$v_\lambda=\exp(\alpha:s_\lambda)\pmod{n}$，

を計算して、(s_λ, v_λ)を利用者λに安全に配布する。ただし、$M=l.c.d(\xi_1-1, \xi_2-1, \eta_1-1, \eta_2-1)$，$N=l.c.d(q-1, q'-1)$。

【0145】このとき、

【0146】

【数112】$s_\lambda\neq s_\mu$ and $v_\lambda\neq v_\mu$ if $I_\lambda\neq I_\mu\in\Lambda=Z/(N)$，

が成立することに注意する。

【0147】③マスタ鍵の共有

ネットワークの利用者λは、ベクトル(y_λ, v_λ)をλの公開鍵として登録を行なう。

【0148】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文Mを鍵Kで暗号化した結果および復号化した結果をそれぞれE(K;M)，D(K;M)で表わす。

【0149】ネットワークの利用者A，Bについて、AはBに対して電子メールを送りたい。この目的の下で、A，Bは次の手順を実行する

AはAの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵（x_A，s_A）とBの公開鍵（y_B，v_B）からマスタ鍵$K_{A.B}$を、

27

【０１５０】

【数113】$K_{A.B}=g(\phi(\exp(y_B:x_A)\pmod p),\exp(v_B:s_A)\pmod n))$，

にて作成する。同様に、ＢはＢの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵（x_B，s_B）とＡの公開鍵（y_A，v_A）からマスタ鍵$K_{B.A}$を、

$$\phi:Z/(p)\times Z/(n)\rightarrow Z/(m)\quad((x,x)\rightarrow x),$$

なる同型写像を表わす（$m=pn$）。ここで、ｘはそれぞれの剰余環におけるｘを代表元とする剰余類を表わす。

【０１５３】このとき、明らかに、$K_{A.B}=K_{B.A}$，が成立する。

【０１５４】さらに、Ａは電子メールを送信する機会が多い利用者については、それらの利用者とＡとの間の各マスタ鍵の集合S_A、または、Ａの秘密情報x_Aから利用者側装置100A内の鍵生成器103Aにより鍵Ｋ（Ａ）を作成し、暗復号化装置105Aを用いて鍵Ｋ（Ａ）によりS_Aを暗号化したＣ（Ａ）＝Ｅ（Ｋ（Ａ）；S_A），を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【０１５５】④メール本文の暗号化

Ａは、利用者側装置100A内の乱数発生器101Aを用いて乱数ｒを選び、ｒを入力として鍵生成器103Aからデータ暗号化鍵ｋを作成する。メール本文Ｐを暗復号化装置105Aを用いてデータ暗号化鍵ｋにより暗号化した暗号文C_1を、$C_1=E(k;P)$，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵ｋをマスタ鍵$K_{A.B}$で暗号化した暗号文C_2を、$C_2=E(K_{A.B};k)$，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵ｋをマスタ鍵$K_{A.B}$で暗号化した暗号文C_2を、$C_2=E(K_{A.B};k)$，にて作成する。

【０１５６】Ａは、通信装置108Aを用いてC_1とC_2をＢに送る。

【０１５７】⑤メール本文の復号化

Ｂは送られてきたC_1とC_2に対して、Ｂの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B.A}$より、$k=D(K_{B.A};C_2)$，にてデータ暗号化鍵ｋを復号化し、次にデータ暗号化鍵ｋを用いて、$P=D(k;C_1)$，にて、メール本文Ｐを復号化する。

【０１５８】（実施例６）実施例６は実施例３の拡張版であり、αの値を秘密にすることにより安全性をさらに向上させている。

【０１５９】①準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。ただし、関数ｆは秘密鍵作成装置203内に格納されてい

28

＊【０１５１】

【数114】$K_{B.A}=g(\phi(\exp(y_A:x_B)\pmod p),\exp(v_A:s_B)\pmod n))$，

にて計算する。ただし、ｇはハッシュ計算器内で用いられるハッシュ関数を表わし、ϕは，

【０１５２】

【数115】

$$\phi:Z/(p)\times Z/(n)\rightarrow Z/(m)\quad((x,x)\rightarrow x),$$

るものとする。

【０１６０】公開情報：

・ｐ；素数，

・$n=q\cdot q'$，

・$a\in Z$ s.t $0<a<p$、かつ、ａは$Z/(p)$で原始根，

秘密情報：

・ｑ，$q'\in Z$；素数 s.t $q-1=2\xi_1\xi_2$，$q'-1=2\eta_1\eta_2$（ξ_1，ξ_2，η_1，η_2；素数），

・$\alpha\in Z$ s.t αは$Z/(q)$，$Z/(q')$で原始根．

・ｆ；擬似ランダム関数．

ネットワークの各利用者λは利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【０１６１】秘密鍵：

【０１６２】

【数116】・$x_\lambda\in Z$ s.t $0<x_\lambda<p-1$．

公開鍵：

【０１６３】

【数117】・$y_\lambda=\exp(a:x_\lambda)\pmod p$．

②センタへの登録

ネットワークの利用者λはセンタに自分のＩＤ情報I_λを登録する。

【０１６４】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、利用者λのＩＤ情報I_λに対して、

（１）$I_\lambda+i_\lambda\pmod N$は平方剰余、

（２）$I_\lambda+i_\lambda\pmod N\neq I_\mu+i_\mu\pmod N$ if $\lambda\neq\mu$、

となるように正整数i_λを選び、

【０１６５】

【数118】$s_\lambda=\exp(I_\lambda+i_\lambda:1/2)\pmod N$，

$v_\lambda=\exp(\alpha:s_\lambda)\pmod n$，

を計算して、（s_λ，v_λ）を利用者λに安全に配布する。

【０１６６】このとき、明らかに、$s_\lambda\neq s_\mu$，$v_\lambda\neq v_\mu$ if $\lambda\neq\mu$，が成立する。

【０１６７】③マスタ鍵の共有

ネットワークの利用者λは、ベクトル（y_λ，v_λ）をλの公開鍵として登録を行なう。

【０１６８】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アル

29

ゴリズムを用いて平文Mを鍵Kで暗号化した結果および復号化した結果をそれぞれE(K；M)，D(K；M)で表わす。

【0169】ネットワークの利用者A，Bについて、AはBに対して電子メールを送りたい。この目的の下で、A，Bは次の手順を実行する

AはAの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Aの秘密鍵（x_A，s_A）とBの公開鍵（y_B，v_B）からマスタ鍵$K_{A,B}$を、

【0170】

【数119】$K_{A,B}=g(\phi(\exp(y_B : x_A) \pmod p), \exp *$

$\phi : Z/(p) \times Z/(n) \rightarrow Z/(m)$

なる同型写像を表わす（$m=pn$）。ここで、xはそれぞれの剰余環におけるxを代表元とする剰余類を表わす。

【0173】このとき、明らかに、$K_{A,B}=K_{B,A}$，が成立する。

【0174】さらに、Aは電子メールを送信する機会が多い利用者については、それらの利用者とAとの間の各マスタ鍵の集合S_A、または、Aの秘密情報x_Aから利用者側装置100A内の鍵生成器103Aにより鍵K(A)を作成し、暗復号化装置105Aを用いて鍵K(A)によりS_Aを暗号化したC(A)＝E(K(A)；S_A)，を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【0175】④メール本文の暗号化

Aは、利用者側装置100A内の乱数発生器101Aを用いて乱数rを選び、rを入力として鍵生成器103Aからデータ暗号化鍵kを作成する。メール本文Pを暗復号化装置105Aを用いてデータ暗号化鍵kにより暗号化した暗号文C_1を、$C_1=E(k；P)$，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵kをマスタ鍵$K_{A,B}$で暗号化した暗号文C_2を、$C_2=E(K_{A,B}；k)$，にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵kをマスタ鍵$K_{A,B}$で暗号化した暗号文C_2を、$C_2=E(K_{A,B}；k)$，にて作成する。

【0176】Aは、通信装置108Aを用いてC_1とC_2をBに送る。

【0177】⑤メール本文の復号化

Bは送られてきたC_1とC_2に対して、Bの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B,A}$より、$k=D(K_{B,A}；C_2)$，にてデータ暗号化鍵kを復号化し、次にデータ暗号化鍵kを用いて、$P=D(k；C_1)$，にて、メール本文Pを復号化する。

【0178】（実施例7）実施例7は実施例4の拡張版であり、αの値を秘密にすることにより安全性をさらに

30

＊($v_B : s_A$) (mod n))，

にて作成する。同様に、BはBの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵（x_B，s_B）とAの公開鍵（y_A，v_A）からマスタ鍵$K_{B,A}$を、

【0171】

【数120】$K_{B,A}=g(\phi(\exp(y_A : x_B) \pmod p), \exp(v_A : s_B) \pmod n))$，

にて計算する。ただし、gはハッシュ計算器内で用いられるハッシュ関数を表わし、φは，

【0172】

【数121】

$((x, x) \rightarrow x)$，

向上させている。

【0179】①準備

センタはセンタ側装置200内の素数発生器201、原始根生成器202および演算器204を用いて次の情報を作成する。

【0180】公開情報：

・p；素数，

・$n=q \cdot q'$（q，q'；素数），

・$a \in Z$ s.t $0<a<p$、かつ、aはZ/(p)で原始根，

秘密情報：

・Z/(N)の元を出力する秘密鍵暗号アルゴリズムおよび鍵r，

・$\alpha \in Z$ s.t αはZ/(q)，Z/(q')で原始根.

ここで、$N=l.c.d(q-1, q'-1)$とする。また、センタの秘密情報である秘密鍵暗号アルゴリズムにより、平文Mを鍵kで暗号化および復号化した結果をそれぞれ$E_0(k；M)$，$D_0(k；M)$で表わす。

【0181】ネットワークの各利用者λは利用者側装置100内の乱数発生器101およびべき乗算器102を用いて次の鍵を作成する。

【0182】秘密鍵：

【0183】

【数122】・$x_\lambda \in Z$ s.t $0<x_\lambda<p-1$.

公開鍵：

【0184】

【数123】・$y_\lambda=\exp(a : x_\lambda) \pmod p$.

②センタへの登録

ネットワークの利用者λはセンタに自分のID情報I_λを登録する。

【0185】センタはセンタ側装置200内の秘密鍵作成装置203を用いて、利用者λのID情報I_λに対して、

【0186】

【数124】$s_\lambda=E_0(r；I_\lambda) \in Z/(N)$，

$v_\lambda=\exp(\alpha : s_\lambda) \pmod N$，

を計算して、（s_λ，v_λ）を利用者λに安全に配布する。

【0187】このとき、$s_\lambda \neq s_\mu$ and $v_\lambda \neq v_\mu$ i

31

ｆ Ｉλ≠Ｉμ∈Λ＝Ｚ/(Ｎ)，が成立することに注意する。

【０１８８】③マスタ鍵の共有

ネットワークの利用者λは、ベクトル（ｙλ，ｖλ）をλの公開鍵として登録を行なう。

【０１８９】さらに、ネットワークに接続された利用者側装置100内には同一の秘密鍵暗号系アルゴリズムを内蔵した暗復号化装置105があり、この秘密鍵暗号系アルゴリズムを用いて平文Ｍを鍵Ｋで暗号化した結果および復号化した結果をそれぞれＥ(Ｋ；Ｍ)，Ｄ(Ｋ；Ｍ)で表わす。

【０１９０】ネットワークの利用者Ａ，Ｂについて、ＡはＢに対して電子メールを送りたい。この目的の下で、Ａ，Ｂは次の手順を実行する

ＡはＡの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Ａの秘密鍵 ＊

$$\phi : Z/(p) \times Z/(n) \rightarrow Z/(m)$$

なる同型写像を表わす（ｍ＝ｐｎ）。ここで、ｘはそれぞれの剰余環におけるｘを代表元とする剰余類を表わす。

【０１９４】このとき、明らかに、$K_{A.B}=K_{B.A}$，が成立する。

【０１９５】さらに、Ａは電子メールを送信する機会が多い利用者については、それらの利用者とＡとの間の各マスタ鍵の集合S_A、または、Ａの秘密情報x_Aから利用者側装置100A内の鍵生成器103Aにより鍵Ｋ(Ａ)を作成し、暗復号化装置105Aを用いて鍵Ｋ(Ａ)によりS_Aを暗号化したＣ(Ａ)＝Ｅ(Ｋ(Ａ)；S_A)，を、メモリ107Aに記憶する。以後の電子メール通信において、データ暗号化鍵更新のためなどでマスタ鍵が必要な場合、マスタ鍵が記憶されているものについては、新たに自分の秘密鍵と相手の公開鍵からマスタ鍵を作成することなく、メモリ107Aに記憶されているマスタ鍵を使う。

【０１９６】④メール本文の暗号化

Ａは、利用者側装置100A内の乱数発生器101Aを用いて乱数ｒを選び、ｒを入力として鍵生成器103Aからデータ暗号化鍵ｋを作成する。メール本文Ｐを暗復号化装置105Aを用いてデータ暗号化鍵ｋにより暗号化した暗号文C_1を、C_1＝Ｅ（ｋ；Ｐ），にて作成する。さらに、暗復号化装置105Aを用いてデータ暗号化鍵ｋをマスタ鍵$K_{A.B}$で暗号化した暗号文C_2を、C_2＝Ｅ($K_{A.B}$；ｋ)，にて作成する。

【０１９７】Ａは、通信装置108Aを用いてC_1とC_2をＢに送る。

【０１９８】⑤メール本文の復号化

Ｂは送られてきたC_1とC_2に対して、Ｂの利用者側装置100B内の暗復号化装置105Bを用いて、まず、マスタ鍵$K_{B.A}$より、ｋ＝Ｄ($K_{B.A}$；C_2)，にてデータ暗号化鍵ｋを復号化し、次にデータ暗号化鍵ｋを用いて、Ｐ＝Ｄ(ｋ；C_1)，にて、メール本文Ｐを復号化する。

32

＊（x_A，s_A）とＢの公開鍵（y_B，v_B）からマスタ鍵$K_{A.B}$を、

【０１９１】

【数125】$K_{A.B}=g(\phi(\exp(y_B : x_A) \pmod p), \exp(v_B : s_A) \pmod n))$，

にて作成する。同様に、ＢはＢの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵（x_B，s_B）とＡの公開鍵（y_A，v_A）からマスタ鍵$K_{B.A}$を、

【０１９２】

【数126】$K_{B.A}=g(\phi(\exp(y_A : x_B) \pmod p), \exp(v_A : s_B) \pmod n))$，

にて計算する。ただし、ｇはハッシュ計算器内で用いられるハッシュ関数を表わし、φは，

【０１９３】

【数127】

$((x, x) \rightarrow x)$，

【０１９９】（実施例８）実施例１から実施例７において、以下のようにメール本文の暗号化およびメール本文の復号化を行なう。

【０２００】・メール本文の暗号化

Ａは、利用者側装置100A内の乱数発生器101Aを用いて乱数ｒを選び、ｒを入力として鍵生成器103Aからデータ暗号化鍵ｋを作成する。メール本文Ｐを暗復号化装置105Aを用いてデータ暗号化鍵ｋにより暗号化した暗号文C_1を、C_1＝Ｅ（ｋ；Ｐ），にて作成する。さらに、演算器を用いてデータ暗号化鍵ｋとマスタ鍵$K_{A.B}$の排他的論理和を、C_2＝ｋ＊$K_{A.B}$，にて作成する。

【０２０１】Ａは通信装置108Aを用いてC_1とC_2をＢに送る。

【０２０２】・メール本文の復号化

Ｂは送られてきたC_1とC_2に対して、まず、演算器104Bを用いてマスタ鍵$K_{B.A}$とC_2の排他的論理和を計算することによりデータ暗号化鍵ｋを復号化する。すなわち、ｋ＝C_2＊$K_{A.B}$．次に、暗復号化装置105Bを用いてデータ暗号化鍵ｋから、Ｐ＝Ｄ(ｋ；C_1)，にてメール本文Ｐを復号化する。

【０２０３】（実施例９）実施例２から実施例８のマスタ鍵共有において、ＡはＡの利用者側装置100A内のべき乗算器102Aと演算器104Aとハッシュ計算器106Aを用いて、Ａの秘密鍵（x_A，s_A）とＢの公開鍵（y_B，v_B）からマスタ鍵$K_{A.B}$を、

【０２０４】

【数128】$K_{A.B}=g((\exp(y_B : x_A) \pmod p) * (\exp(v_B : s_A) \pmod n))$，

にて作成する。同様に、ＢはＢの利用者側装置100B内のべき乗算器102Bと演算器104Bとハッシュ計算器106Bを用いて、自分の秘密鍵（x_B，s_B）とＡの公開鍵（y_A，v_A）からマスタ鍵$K_{B.A}$を、

【０２０５】

33

【数129】$K_{B,A}=g((\exp(y_A:x_B)\pmod p))*(\exp(v_A:s_B)\pmod n))$,
にて計算する。ただし、ｇはハッシュ計算器内で用いられるハッシュ関数を表わし、ｘ＊ｙはｘとｙの排他的論理和を表わす。

【０２０６】（実施例１０）ネットワークの各利用者はカード400を所持し、電子メール通信時にはカード400を利用者側装置500内のカード読取装置501に差し込み、実施例１から実施例９において、利用者側装置100内の乱数発生器101、べき乗算器102、鍵生成器103、演算器104、暗復号化装置105、ハッシュ計算器106、メモリ107を用いて行なう処理をそれぞれカード400内の乱数発生器401、べき乗算器402、鍵生成器403、演算器404、暗復号化装置405、ハッシュ計算器406、メモリ407を用いて行ない、受信者への送信文はカード400内の出力装置408を用いて、利用者側装置500内のカード読取装置501に出力され、さらに、利用者側装置500内の通信装置502を用いて通信回線300を介して送信する。

【０２０７】

【発明の効果】本発明における電子メール暗号化方法によれば、メールシステムや機種に特定しないで通常のメールと併用できる特徴を有するため、通信ネットワークの形態に依らず適用が可能である。また、電子メールの送信者および受信者はそれぞれ自分の秘密鍵と相手の公開鍵からマスタ鍵の共有を行ない、秘密鍵暗号を用いてメール本文の暗号化およびデータ暗号化鍵配送を行なっているため、送受信者双方の計算処理負担が少なく高速な暗号化処理が可能となった。また、ディジタル署名などの付加情報を付けることなく送信者の認証が可能となるため、メール暗号文のヘッダ情報が少なく、電子メー

34

ルのセキュリティ機能実現のための処理時間が大幅に削減された。さらに、ＩＤ情報は利用者毎に異なることを利用して、センタと利用者が協力して利用者の鍵生成を行なうことにより、利用者の鍵の一致の心配がなく、盗聴や不正者のなりすまし対して高い安全性を実現した。

【図面の簡単な説明】

【図１】本発明の実施例におけるシステム構成を示すブロック図。

【図２】本発明の電子メール暗号化方法の概念を示す説明図。

【図３】実施例１から９のシステム構成内の利用者側装置内部構成を示すブロック図。

【図４】実施例１から９のシステム構成内のセンタ側装置内部構成を示すブロック図。

【図５】実施例１０のシステム構成内のカード内部構成を示すブロック図。

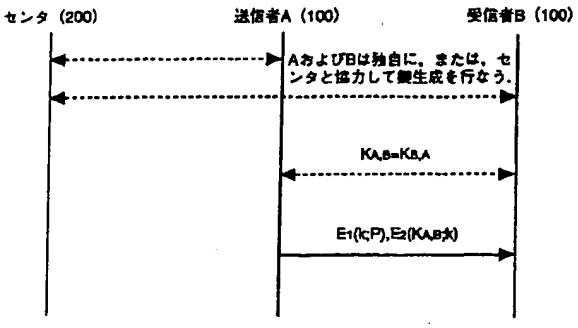
【図６】実施例１０のシステム構成内の利用者側装置内部構成を示すブロック図。

【符号の説明】

100…利用者側装置、
101…利用者側装置100内の乱数発生器、
102…利用者側装置100内のべき乗算器、
103…利用者側装置100内の鍵生成器、
104…利用者側装置100内の演算器、
105…利用者側装置100内の暗復号化装置、
106…利用者側装置100内のハッシュ計算器、
107…利用者側装置100内のメモリ、
108…利用者側装置100内の通信装置、
200…センタ側装置。

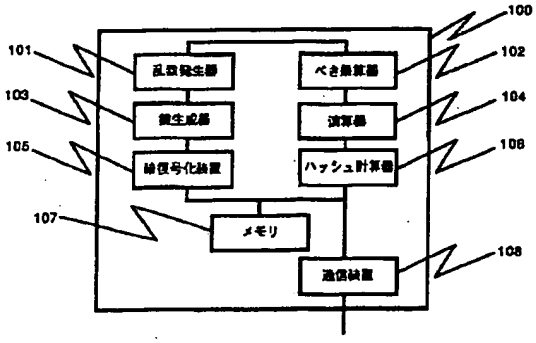
【図２】

図 2



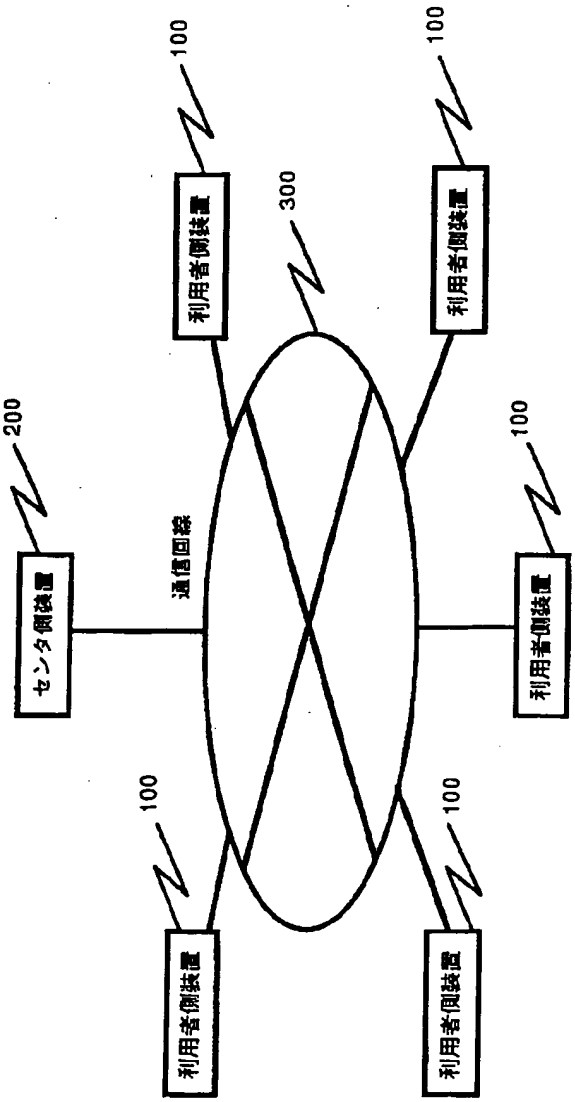
【図３】

図 3



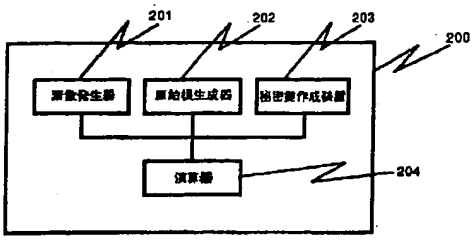
【図１】

図　１


100
100
利用者側装置
利用者側装置
300
200
通信回線
センタ側装置
100
利用者側装置
100
100
利用者側装置
利用者側装置

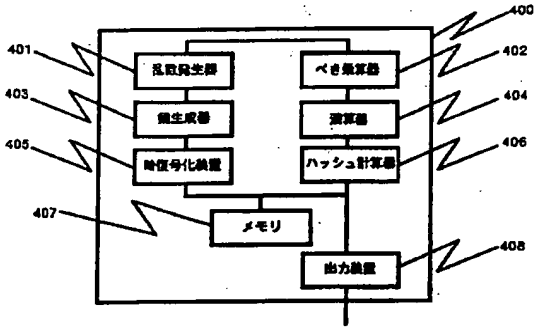
【図４】

図 4



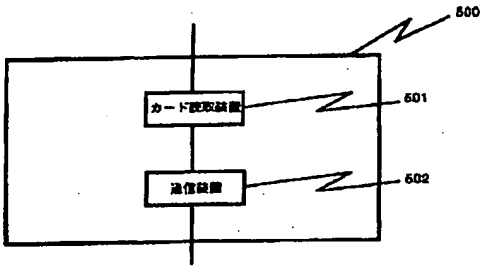
【図５】

図 5



【図６】

図 6



フロントページの続き

(51) Int. Cl.⁶	識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ　12/58				